Device and method for authorizing a user to get access to content stored in encrypted form on a storage medium

The present invention relates to a device and a corresponding method for authorizing a user to get access to content stored in encrypted form on a storage medium, said storage medium storing a machine-readable medium identifier and at least one key table encrypted by use of a key table key and storing at least one asset key for decrypting encrypted content. The invention relates further to a network in which said method is employed as well as to a computer program for implementing said method.

European patent application 02 078 437.7 (PHNL020775) describes a method of protecting content stored on a storage medium against unauthorized access, said storage medium being accessible by a drive of a portable device which is connectable to a network. In order to provide a high level of protection against unauthorized access, the authentication procedure of the network is used to generate a cryptographic key, hereinafter called asset key, for encryption and decryption of content stored on said storage medium. In particular, it describes the use of this method in a mobile phone network where the authentication key is stored on a SIM card used in a mobile phone. Thus, the main idea is that the storage medium contains a unique medium identifier and that the mobile communication network authentication procedure is used to transform this medium identifier into the actual asset key. This transform is performed by the user's SIM card, when used in a mobile phone network, so that without this SIM card the content of the storage medium can not be read. This provides a very simple and secure way for users to protect their private content, also referred to as SIM encryption method in the following.

A drawback of this approach is that access to the content is restricted to a single user, or more particularly, to a single user's SIM card. It is thus an object of the present invention to provide a device and method which allow the user to provide access to the content to other users in a simple, but still secure way. Further, transparent access from different devices owned by the same user, for instance from different mobile phones having

different SIM cards, shall be enabled. A corresponding network and a computer program for implementing said method shall be provided as well.

This object is achieved according to the present invention by a device as claimed in claim 1 comprising:

- a connection means for connecting said device to a network,
- a drive for accessing said storage medium, in particular for reading content and said medium identifier from said storage medium, and
- a transmitter for transmitting said medium identifier and a user identifier of a user, who shall be authorized to get access to said content and who is identified to said network by said user identifier, to an authentication unit within said network, said medium identifier and said user identifier being used by said authentication unit for generating a key table key for said user enabling said user to decrypt at least one predetermined key table.

A corresponding method is defined in claim 9. A computer program for implementing said method is defined in claim 11. A network in which the invention is employed is defined in claim 10 and comprises:

- a first user device for authorizing a user of a second user device to get access to content stored in encrypted form on a storage medium, said storage medium storing a machine-readable medium identifier and at least one key table encrypted by use of a key table key and storing at least one asset key for decrypting encrypted content, said first user device comprising:
  - a connection means for connecting said device to a network,
  - a drive for accessing said storage medium, in particular for reading content and said medium identifier from said storage medium, and
  - a transmitter for transmitting said medium identifier and a user identifier of a user, who shall be authorized to get access to said content and who is identified to said network by said user identifier, to an authentication unit within said network;
- an authentication unit comprising:
  - a receiver for receiving said medium identifier and said user identifier,
  - a key generating means for generating a key table key for said user using said medium identifier and said user identifier, said key table key enabling said user to decrypt said at least one key table, and
  - a transmitter for transmitting said key table key to said first and/or said second user device; and

- a second user device of a user who shall be authorized to get access to content stored in encrypted form on said storage medium comprising:

- a connection means for connecting said device to said network,

- a receiver for receiving said key table key from said authentication unit or said first user device,

- a drive for accessing said storage medium, in particular for reading content from said storage medium, and for decrypting at least one predetermined key table using the received key table key.

The present invention is based on the idea to use the authentication process of a network for enabling a user who has access to content stored on a storage medium to authorize other users to get access to the same content. By use of the medium identifier and the user identifier of a user who shall be authorized the authentication unit of the network generates and provides a key table key. This key table key can then be used by the user to be authorized to decrypt an assigned and predetermined key table provided for this "new" user in which key table an asset key is stored for decryption of the content to which he shall get access. Thus, "new" users can be added to an authorization list without their direct involvement. This method is simple and easy to implement, but nevertheless provides a high level of security due to the use of the very secure authentication procedure of the network for generating key table keys allowing access to key tables and thus to asset keys for decrypting content.

The network proposed according to the present invention, which is preferably a communication network such as a GSM or an UMTS network, comprises at least two user devices, which may both belong to the same user or to different users, and an authentication unit for authenticating users when they connect to the network. The authentication procedure used for authenticating users is very secure since breaking the authentication algorithm used in a mobile communication network would allow the user to make calls that would be billed to other users. Therefore, the level of protection of such an authentication algorithm is very high and is considered to be sufficient for protecting the user's data when using the authentication algorithm for generating key table keys as proposed according to the present invention. Furthermore, said authentication unit is also used for generating asset keys as described in the above mentioned European patent application 02 078 437.7 (PHNL020775). The description of this method in this document is herein incorporated by reference.

Preferred embodiments of the invention are defined in dependent claims. According to an embodiment the device further comprises a receiver for receiving the key

table key for the user to be authorized from the network, and the transmitter is operative for transmitting the received key table key to said user. Thus, the user who wants to authorize another user to have access to content communicates with the network to get a new key table key for the other user which is then received by him and forwarded to the other user, for instance in the form of an SMS or any other electronic message. The user to be authorized is thus not involved in the procedure of generating the new key table key.

According to another embodiment the new key table key may also be provided directly from the network to the user to be authorized. To identify this user the network can use the user identifier already provided by the first user together with a medium identifier to the authentication unit for generation of the key table key.

According to a further embodiment the storage medium not only stores one single key table but a plurality of key tables, for instance one key table for each user. Moreover, to each key table a user check identifier might be assigned, which is checked by the device prior to decryption to find the right key table assigned to said user. This avoids decryption of a number of (or even all) key tables in order to find the correct key table for the user. The user check identifier could, for instance, be identical to the user identifier identifying the user to the network, for instance, as claimed in a further dependent claim when being employed in a mobile communication network, the international mobile subscriber identity (IMSI) or the telephone number of said user.

If it is desirable to hide the user's identity, this user check identifier can also be encrypted, for instance in a very simple way by use of an XOR function with the user's key table key. This would mean that again this encrypted user check identifier has to be decrypted, in particular for a number or all tables. However, this operation is very simple and not much time-consuming. Since each user check identifier is encrypted with a different key (the key table keys of different users), it is no easy to determine the underlying user check identifier, so that even such a simple encryption, e.g. the use of a symbol XOR function, should be sufficiently secure.

In order to see if the correct key table has been decrypted and if the decryption has been correctly done, each key table may further comprise a decryption check identifier as proposed according to another embodiment. For said check an appropriate decryption check means may by provided in the user device. In addition, some randomly generated patting fields may be provided in order to make hacking more difficult. In a preferred embodiment, the user check identifier is used also as decryption check identifier, for instance, once

unencrypted on the outside to identify the user belonging to the key table, and twice inside the key table, i.e. encrypted, to check whether the decryption was correct.

In a simple embodiment there is only one key table provided on the storage medium, and the first user who wants to authorize a second user provides his own key table key to the second user enabling him to decrypt the same key table. Alternatively, for each user there may be provided a separate key table on the storage medium each being decrypted by a different key table key. For generating such key tables appropriate key table generating means are provided according to another embodiment. The first user thus uses a key table key to encrypt the asset key which allows decryption of the content to which the other user shall get access and thus generates a key table which is then stored by said accessing means on the storage medium.

Thus, according to a preferred aspect of the invention each item of content is encrypted in its own asset key. which can be any random key; these asset keys are stored in a key table. The first user uses known SIM encryption method (e.g. using his SIM card) to get his key table key, which is the key used to encrypt the key table. The encrypted-asset keys and key table are stored on the medium. If the first user wants to access the asset keys he needs to use the SIM encryption method again to get his key table key. Other users get other keys using the SIM encryption method because their SIM is different. If the first user wants a second user to have access tot the content, then the first user encrypts the key table with the asset keys in the SIM derived key of the second user. Now a second encrypted key table is stored on medium, but not the SIM derived key itself.

Preferably, as mentioned above, the invention is employed in a mobile communication network and the user device is a mobile phone. The authentication algorithm used for authenticating mobile communication devices to the network is then employed for generating the key table keys and, preferably, also the asset keys (actually any random key will do).

When the network is a mobile communication network the authentication unit of the home location register (HLR) of the user to be authorized is used for generating the key table key for said user for transmission of the medium identifier and the user identifier to the authentication unit. Also for transmission of the generated key table key to the user device a secure channel can be implemented. Preferably, the authentication procedure is then also used to generate the key for the secure channel in a similar way as used for generating the key table key.

It is also preferred that the mobile network operator can offer the above described procedure as a service. Users from different networks can also be authorized in the same way in which the network handles roaming users. Moreover, by offering this service, but not supporting users from other networks, the network can also encourage users of different networks to subscribe to this network.

The invention will now be explained in more detail with reference to the drawings in which

Fig. 1 shows an embodiment of a record carrier according to the invention,

Fig. 2 shows an embodiment of a network according to the present invention,

Fig. 3 shows a flow chart illustrating the method according to the invention, and

Fig. 4 shows an embodiment of a user device according to the present invention.

Fig. 1 shows a storage medium 10 according to the present invention and illustrates what is stored on such a record carrier. For the following description it is assumed that a particular user of a first user device has access to content which is stored in encrypted form on a record carrier 10, for instance an optical record carrier such as a CD, DVD or BD, which is readable by the user device, which may, for instance, be a portable mobile phone having a drive for accessing the record carrier 10. It is further assumed that the record carrier 10 - besides the encrypted content - stores a machine-readable medium identifier id and at least one key table KL, which is encrypted by use of a key table key KLK and which stores at least one asset key AK. Said asset key AK has been used for encrypting the content C and thus needs to be used by a user for decrypting the encrypted content C.

There might also be more than one key table KL stored on the record carrier 10, in particular one key table KL for each separate user, and each key table KL might be encrypted by a different key table key KLK. Moreover, each key table KL might store more than one asset key AK for decrypting different portions of content C stored on the record carrier 10. Further, to each key table there might be a user check identifier UC assigned for finding the right key table KL and/or each key table might comprise a decryption check

identifier DC for seeing if a key table KL has been correctly decrypted, which will be both explained below in more detail.

Fig. 2 shows an embodiment of a network according to the present invention illustrating the general use of the invention. Fig. 3 illustrates the steps of the method according to the invention as a flow chart. In the network illustrated in Fig. 2 a mobile communication network, in particular a GSM network 3, is shown as an example to which two user devices 1, 2, here two mobile phones, are connectable and over which they can communicate with each other and with other users. The mobile phones 1, 2 each comprise a SIM card reader 4 for reading a SIM card 20. On the SIM card 20 an authentication key is stored which is a secret key shared with an authentication center AuC of the GSM network 3 used for authentication of the mobile phones 1, 2 when connecting to the network 3. The mobile phones 1, 2 further comprise a drive 5 for reading data from and/or storing data on a removable storage medium 10, which can, for instance, be a small form factor optical disc drive. The user devices 1, 2 further comprise connection means 6 for connecting to the network 3 including a transmitter 7 for transmitting data and a receiver 8 for receiving data.

As described in the above mentioned European patent application 02 078 437.7 (PHNL 020775) the mobile communication network authentication procedure is used to transform the unique identifier of the record carrier 10 (e.g. a serial number stored in a particular area on the record carrier 10) into the asset key AK used for encryption of the content C (or part of the content) stored on the record carrier 10. This transform is either performed by the SIM card 20 or by the authentication center AuC, so that without this SIM card the content can not be decrypted and read. This provides a very simple and secure way for the user to protect his private content. If the user now desires to allow other users to access his content or to enable transparent access from different devices owned by himself, the following procedure is performed.

In a first step S1 the unique identifier id is read from the record carrier. This medium identifier id and a user identifier ui of a second user who shall be authorized by the first user to get access to a particular piece of the first user's content, are then (S2) transmitted to the authentication center AuC of the network 3. Therein (S3) a key table key KLK, for instance a key locker key in case the key tables are in the form of key lockers, is generated by the key generator 31 from the medium identifier id and the user identifier ui. The generated key table key KLK can then be transmitted back only to the first user device 1 (S4) or both to the first user device 1 and to the second user device 2 (S8).

In the first case the first user device 1 generates now a key table KL2 for the second user 2 (S5) by use of the received key table key KLK, i.e. the asset key(s) which shall be given to the second user for accessing content are encrypted by said key table key KLK. The second user 2 is then authorized by getting the key table key KLK for decrypting the newly generated key table KL2 from the first user (S6). By use of the key table key KLK he is then able to decrypt the key table KL2, read the asset key(s) from it and use the asset key(s) for decryption of content. The user 2 is thus added to the authorization list without direct involvement.

In the second alternative where the key table key KLK is also directly forwarded to the second user (S8), the first user device 1 also generates now a key table KL2 for the second user 2 (S9) by use of the received key table key KLK (identically as in step 5). But, immediately thereafter the second user 2 may directly decrypt the new key table KL2 by use of this key table key KLK (S10).

A further possibility is that a second user has a record carrier for which he does not have access. But he may ask the user who has access via the network to give him access as well. Thus, the first user may provide his key table key to the second user via the network and thus authorize him to access its own key table by use of the same key table key. In this case, it is also sufficient that there is only one single key table stored on the record carrier which is used by all users authorized by the first user 1.

As already mentioned above, each key table KL preferably also comprises a decryption check identifier DC (see Fig. 1) to indicate that the decryption of the key table has worked correctly. To check this the user devices comprise a decryption check unit 9 as shown in the embodiment of the user device 1 illustrated in Fig. 4. Further, the key tables may include some randomly generated padding fields to make hacking more difficult. When a user tries to access the record carrier, the unique identifier id should be transformed using the SIM mapping to an asset key, which is a potential key for decrypting a key table. Using this potential key to decrypt a key table present on the record carrier results in an actual asset key. However, if the user is not authorized then his SIM will generate a key table key, which is, however, not able to correctly decrypt any of the key tables which can be easily seen from the decryption check identifier.

Preferably, as already mentioned, the key tables are key lockers so that different rights can be stored for each user and some content is hidden from some users. The key tables may also be all (for each user) located inside a key locker. The key locker key is then a hidden key on the record carrier.

Furthermore, as also shown in the embodiment of Fig. 4, the user devices may include a user check unit 11 to check a corresponding user check identifier uc preferably stored on the record carrier and assigned to each key table. This user check identifier uc is used to find the correct key table for a user so that decryption of each available key table in order to find the correct one can be avoided. For instance, the user's SIM card contains an identifier to identify the user to the mobile network, called international mobile subscriber identity (IMSI) in GSM, which can used. Alternatively, the user's phone number can be used. Further, if it is desirable to hide the user's identity, this user check identifier uc could be encrypted in a very simple way, e.g. XOR with a key. This means, that again each user check identifier needs to be decrypted by means of a relatively simple XOR operation. Since each user check identifier is preferably XORed with a different key, there is no easy way to determine the underlying user check identifier so that this method may hide the user's identity with sufficient security.

Preferably a user who wants to authorize other users, also generates a new key table for each new user. Therefore, a key table generating unit 12 is also provided in each user device 1 as also shown in Fig. 4.

The user who creates the content will be authorized as indicated in the above mentioned European patent application 02 078 437.7 (PHNL 020775). Adding further users to the authorization list can be done through the network. Therefore, a secure connection is preferably provided between the user device and the network (in particularly the home location register HLR) in GSM of the user to be authorized. As user identifier, again the user's phone number or the user's IMSI can be used. Of course, other user identifiers can be used as well by which the user is uniquely identified to the network.

The authentication procedure described above can also be used to generate the key for a secure channel between the user devices and the network in a similar way.

Preferably, the network operator can offer the above described procedure as a service. Users from different networks can also be authorized in the same way in which the network handles roaming users. However, by offering the service, but not supporting users from other networks, the network can encourage friends or family members of current users to subscribe to their network.

The present invention provides a simple and easily implementable method for adding further users on an authorization list to get access to content belonging to a particular user. The authentication procedure of the network is used in this process which provides a high level of security.